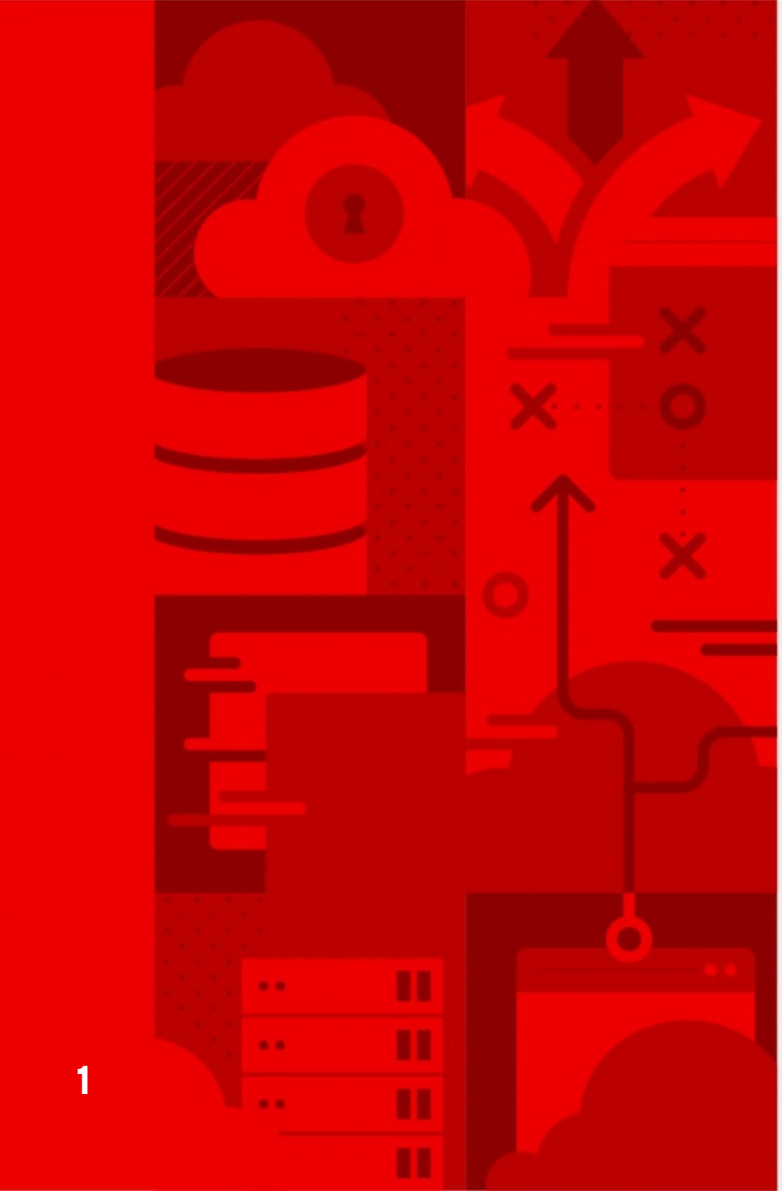


Red Hat
Enterprise Linux 8

システム全体の暗号化ポリシー設定

2019 年 9 月 17 日

レッドハット株式会社
森若 和雄

Red Hat

このスライドについて

対象

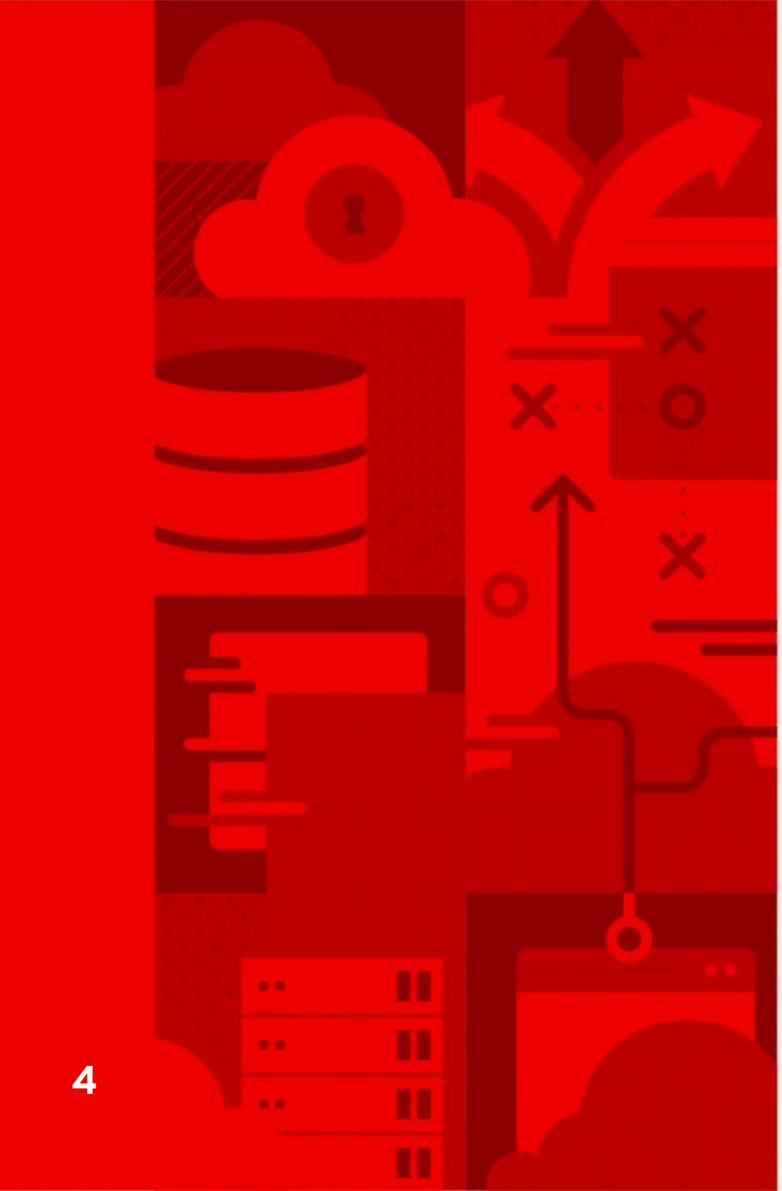
RHEL8 でシステム全体の暗号化ポリシーを設定したい人
RHEL8 の新機能として導入された crypto-policies について知りたい人

目的

crypto-policies の基本的な使い方と、現状の制限を紹介する

概要

- システム全体の暗号化ポリシー設定とは何か？
- crypto-policies の使い方
- crypto-policies 利用時の注意点
- 参考資料



システム全体の暗号化ポリシー設定とは何か？

Red Hat

背景

RHEL が利用する暗号化方式には複数の方式があります

接続時のプロトコル、暗号化のアルゴリズム、署名のアルゴリズム、ハッシュ関数などそれぞれにバリエーションがあります。

暗号化スイートは時とともに弱くなります

コンピュータの高速化や、暗号の研究が進んで攻撃手法が進化することで、暗号を解くために必要な時間が短くなり、やがて実用的な意味がなくなります。
NIST などは推奨する暗号化スイートや、利用すべきでないアルゴリズムなどを発表しています。

(攻撃する側からみると) システムで一番弱い暗号化を利用している箇所がそのシステムの暗号強度

一部で強力な暗号化を利用し、別の箇所では弱い暗号化を利用している場合、一番弱いところを狙われます

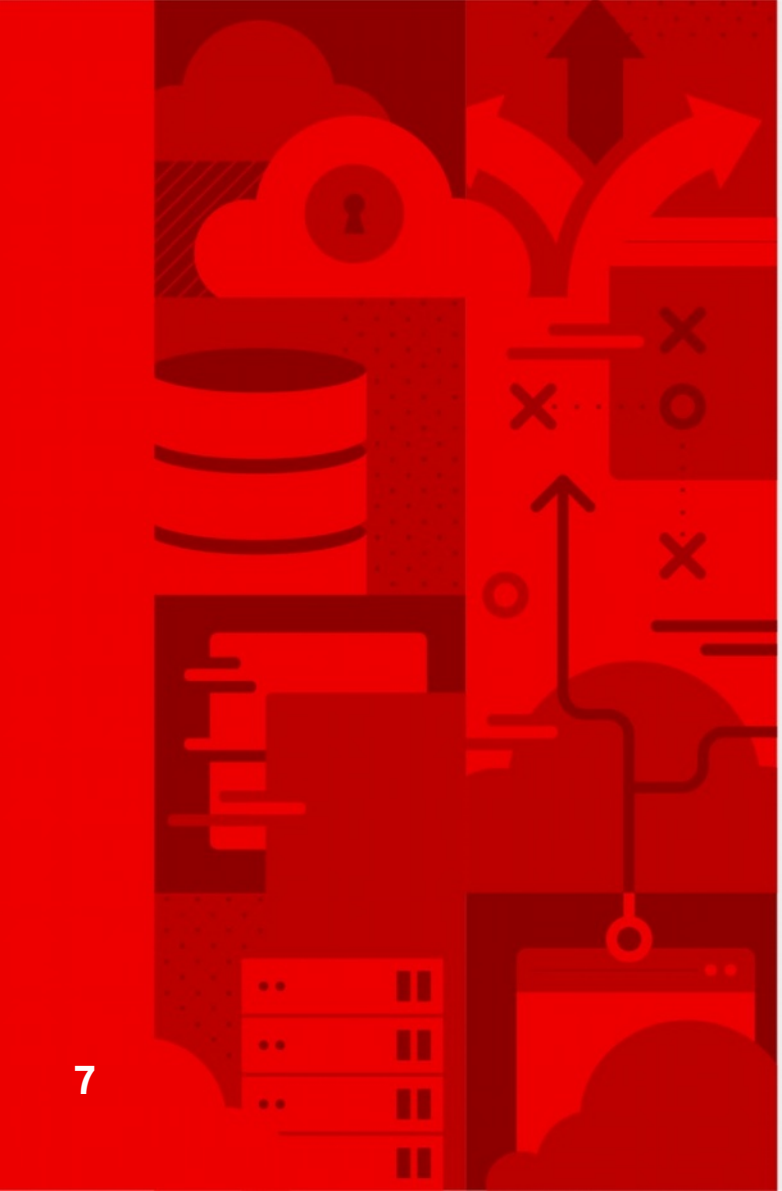
暗号化ポリシーの設定 とは

システム全体の暗号化スイートの設定を一箇所で行う

設定の抜け漏れをなくし、一部の脆弱な設定によりシステム全体が脆弱になる事故を防ぎます

あらかじめ推奨される設定を用意しておく

デフォルトで現在の推奨される設定になります



crypto-policies の使い方

Red Hat

crypto-policies とは何か？

システム全体の暗号化ポリシー設定を行うツール

RHEL8.0 からの新機能です。 GnuTLS, OpenSSL, NSS, OpenJDK, libkrb5, BIND, OpenSSH, libreswan のデフォルトをまとめて設定します。これらのライブラリやアプリケーションのパッケージと連携しています。
(RHEL 8.1 で libssh に対応予定)

あらかじめ定義されたプロファイルから選択する

以下から選択します

- 現在の推奨 (DEFAULT)
- 数年前のシステムとの互換性を提供するためのやや弱い設定 (LEGACY)
- 近い将来でも安全であろう設定 (FUTURE)
- FIPS140-2 要件 (FIPS)

crypto-policies 関連コマンド

管理者が利用するコマンド

- update-crypto-policies

利用例

```
# update-crypto-policies --show
DEFAULT
# update-crypto-policies --set LEGACY
Setting system policy to LEGACY
Note: System-wide crypto policies are applied on application start-up.
It is recommended to restart the system for the change of policies
to fully take place.
```

ポリシーの基本的な選び方

特に何もなければ DEFAULT のまま

DEFAULT ポリシーは現在推奨される暗号化の設定です

古い機器との接続に問題がある場合には LEGACY にする

LEGACY ではセキュリティ上推奨されないプロトコルやアルゴリズムが許可されます

特定の暗号化スイートが指名されている場合には アプリケーションを個別に設定する

crypto-policies のデフォルト設定を無視してアプリケーション毎に設定します。
crypto-policies の upstream を見ると、将来のバージョンではポリシーを独自に作成できるようになりそうです。

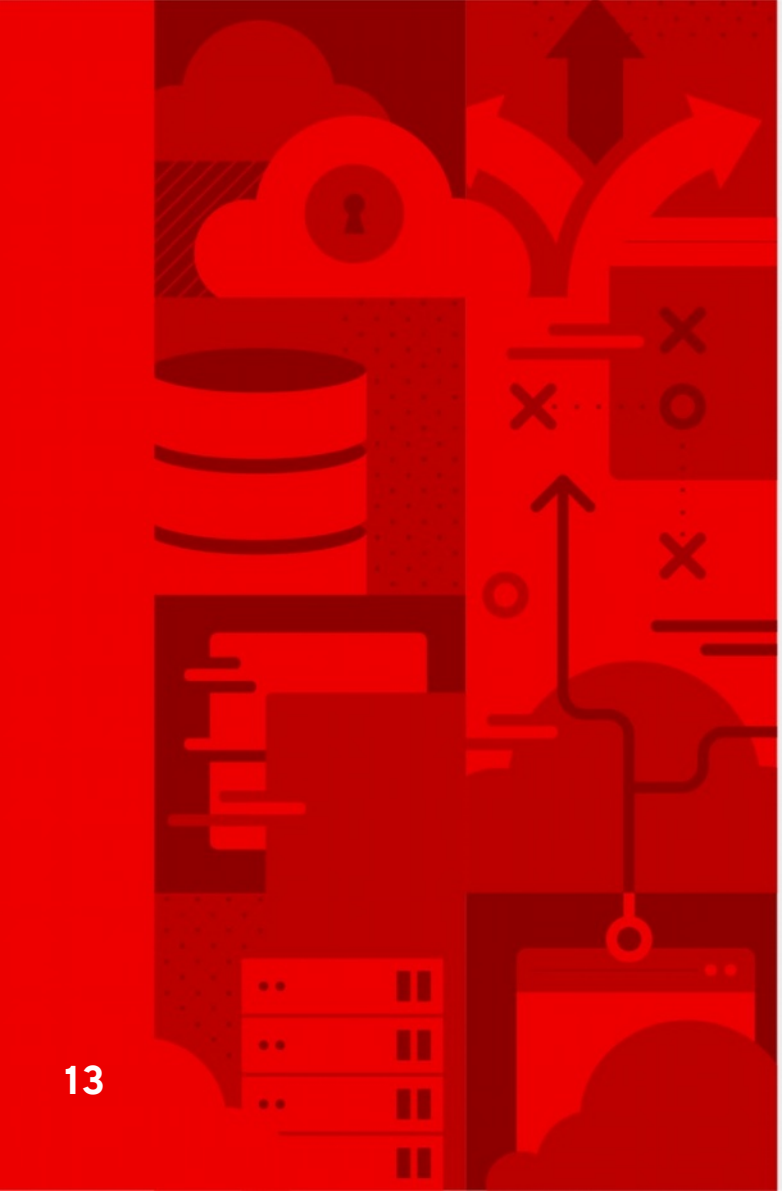
	LEGACY	DEFAULT	FIPS	FUTURE
IKEv1	no	no	no	no
3DES	yes	no	no	no
RC4	yes	no	no	no
DH	min. 1024-bit	min. 2048-bit	min. 2048-bit	min. 3072-bit
RSA	min. 1024-bit	min. 2048-bit	min. 2048-bit	min. 3072-bit
DSA	yes	no	no	no
TLS v1.0	yes	no	no	no
TLS v1.1	yes	no	no	no
SHA-1 デジタル署名	yes	yes	no	no
CBC モード暗号	yes	yes	yes	no
対称暗号 < 256 ビット鍵	yes	yes	yes	no
SHA-1 および SHA-224 の署名を持つ証明書	yes	yes	yes	no

参考 : RHEL8 で利用できないアルゴリズムとプロトコル

RHEL8 から排除された暗号スイートとプロトコル

以下はソースコードに含まれないか、ビルド時に無効にされています。
設定によらず利用できません。

- DES (RHEL 7 以降)
- すべてのエクスポートグレードの暗号化スイート (RHEL 7 以降)
- 署名内の MD5 (RHEL 7 以降)
- SSLv2 (RHEL 7 以降)
- SSLv3 (RHEL 8 以降)
- すべての ECC 曲線 < 224 ビット (RHEL 6 以降)
- すべてのバイナリーフィールドの ECC 曲線 (RHEL 6 以降)



crypto-policies 利用時の注意点

Red Hat

crypto-policies の注意点

crypto-policies は全ての暗号化を網羅できていません

暗号化をあつかう全ての箇所を網羅できていません。 gpg2 、 luks2 など暗号化を扱うが crypto-policies で管理されていないものがあります。

アプリケーション個別での設定でオーバライドされます

crypto-policies は各ライブラリやアプリケーションのデフォルト設定に影響しますが強制力はありません。アプリケーションで明示的に設定が行われると、そちらが優先されます。

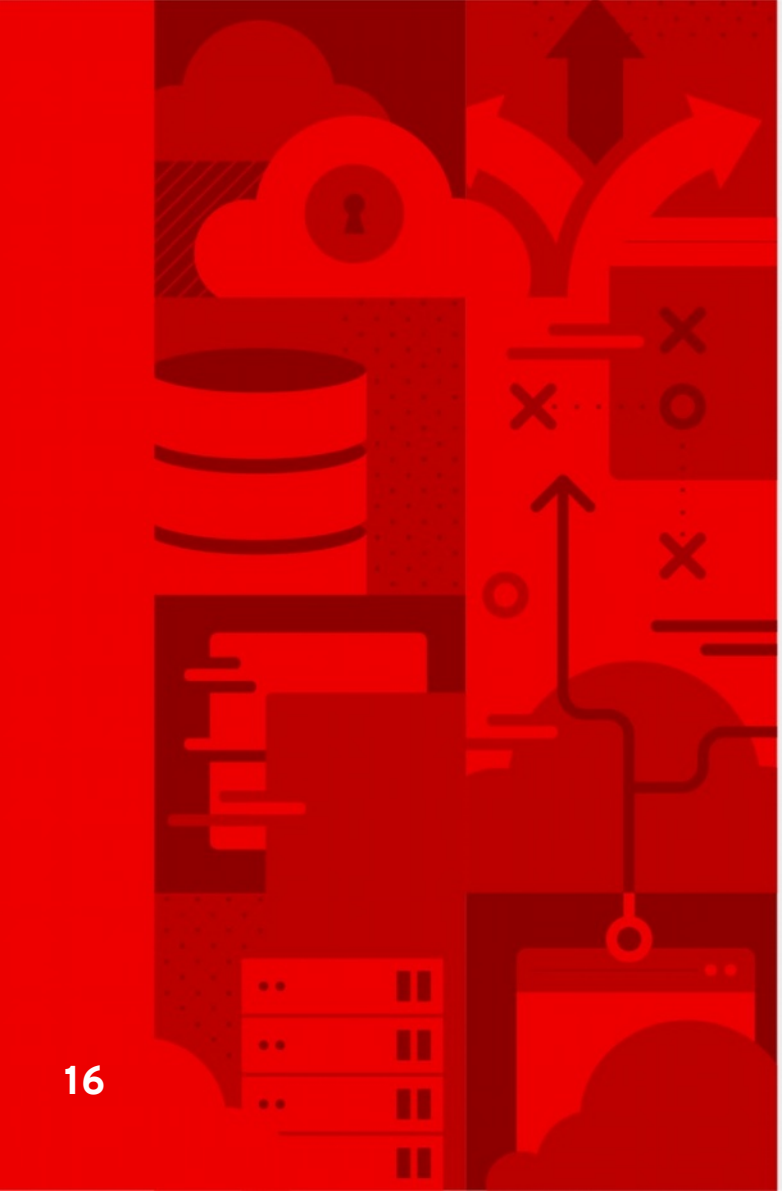
オーバライドしたい場合

一部のソフトウェアは単純に設定を行うだけでオーバライドできないものがあります。 RHEL8 ドキュメント「セキュリティーの強化」内「アプリケーションをシステム全体のポリシーに従わないように除外」を参照ください。

https://red.ht/2l7gxz2

まとめ

- Red Hat Enterprise Linux 8 でシステム全体の暗号化ポリシー設定が追加されました
- 簡単にまとめて設定が可能です
- 通常は DEFAULT と LEGACY のみ考慮すれば十分です
- 個別のアプリケーションでポリシーをオーバライドすることも可能です



参考資料

Red Hat

参考情報

- 公式ドキュメント「セキュリティーの強化」内「システム全体の暗号化ポリシーの使用」
  https://red.ht/2I9j2B5
- fedora-crypto-policies プロジェクトのページ
  https://gitlab.com/redhat-crypto/fedora-crypto-policies

Thank You